

## § 710.34

the procedures of this subpart shall be terminated without a final decision as to the individual's access authorization eligibility, unless a final decision has been rendered prior to the DOE being notified of the change in the individual's pending access authorization status.

[66 FR 47067, Sept. 11, 2001]

### § 710.34 Attorney representation.

In the event the individual is represented by an attorney or other representatives, the individual shall file with the Hearing Officer and DOE Counsel a document designating such attorney or representatives and authorizing one such attorney or representative to receive all correspondence, transcripts, and other documents pertaining to the proceeding under this subpart.

[59 FR 35185, July 8, 1994. Redesignated at 66 FR 47065, Sept. 11, 2001]

### § 710.35 Time frames.

Statements of time established for processing aspects of a case under this subpart are the agency's desired time frames in implementing the procedures set forth in this subpart. However, failure to meet the time frames shall have no impact upon the final disposition of an access authorization by a Manager, Hearing Officer, the Appeal Panel, or the Secretary, and shall confer no procedural or substantive rights upon an individual whose access authorization eligibility is being considered.

[66 FR 47067, Sept. 11, 2001]

### § 710.36 Acting officials.

Except for the Secretary, the responsibilities and authorities conferred in this subpart may be exercised by persons who have been designated in writing as acting for, or in the temporary capacity of, the following DOE positions: The Local Director of Security, the Manager, the Director, Office of Personnel Security, DOE Headquarters, or the General Counsel. The responsibilities and authorities of the Deputy Chief for Operations, Office of Health,

## 10 CFR Ch. III (1–12 Edition)

Safety and Security, may be exercised in his absence only by his designee.

[66 FR 47067, Sept. 11, 2001, as amended at 71 FR 68731, Nov. 28, 2006]

### APPENDIX A TO SUBPART A OF PART 710—SELECTED PROVISIONS OF THE ATOMIC ENERGY ACT OF 1954, AS AMENDED, SEC. 141 (42 U.S.C. 2161), SEC. 145 (42 U.S.C. 2165), SEC. 161 (42 U.S.C. 2201)

(By authority of the Department of Energy Organization Act, 42 U.S.C. 7151(a), the Secretary of Energy or her designated representative is to be substituted for the "Commission" and "General Manager" as appropriate.)

Sec. 141. Policy. It shall be the policy of the Commission to control the dissemination and declassification of Restricted Data in such a manner as to assure the common defense and security. \* \* \*

Sec. 145. Restriction. (a) No arrangement shall be made under section 31, no contract shall be made or continued in effect under section 141, and no license shall be issued under section 103 or 104, unless the person with whom such arrangement is made, the contractor or prospective contractor, or the prospective licensee agrees in writing not to permit any individual to have access to Restricted Data until the Civil Service Commission shall have made an investigation and report to the Commission on the character, associations, and loyalty of such individual, and the Commission shall have determined that permitting such person to have access to Restricted Data will not endanger the common defense and security.

(b) Except as authorized by the Commission or the General Manager upon a determination by the Commission or General Manager that such action is clearly consistent with the national interest, no individual shall be employed by the Commission nor shall the Commission permit any individual to have access to Restricted Data until the Civil Service Commission shall have made an investigation and report to the Commission on the character, associations, and loyalty of such individual, and the Commission shall have determined that permitting such person to have access to Restricted Data will not endanger the common defense and security.

(c) In lieu of the investigation and report to be made by the Civil Service Commission pursuant to subsection (b) of this appendix, the Commission may accept an investigation and report on the character, associations, and loyalty of an individual made by another Government agency which conducts personnel security investigations, provided that a security clearance has been granted to

## Department of Energy

## Pt. 710, Subpt. A, App. A

such individual by another Government agency based on such investigation and report.

(d) In the event an investigation made pursuant to subsections (a) and (b) of this appendix develops any data reflecting that the individual who is the subject of the investigation is of questionable loyalty, the Civil Service Commission shall refer the matter to the Federal Bureau of Investigation for the conduct of a full field investigation, the results of which shall be furnished to the Civil Service Commission for its information and appropriate action.

(e) If the President deems it to be in the national interest he may from time to time determine that investigations of any group or class which are required by subsections (a), (b), and (c) of this appendix be made by the Federal Bureau of Investigation.

(f) Notwithstanding the provisions of subsections (a), (b), and (c) of this appendix, a majority of the members of the Commission shall certify those specific positions which are of a high degree of importance or sensitivity, and upon such certification, the investigation and reports required by such provisions shall be made by the Federal Bureau of Investigation.

(g) The Commission shall establish standards and specifications in writing as to the scope and extent of investigations, the reports of which will be utilized by the Commission in making the determination, pursuant to subsections (a), (b), and (c) of this appendix, that permitting a person access to Restricted Data will not endanger the common defense and security. Such standards and specifications shall be based on the location and class or kind of work to be done, and shall, among other considerations, take into account the degree of importance to the common defense and security of the Restricted Data to which access will be permitted.

(h) Whenever the Congress declares that a state of war exists, or in the event of a national disaster due to enemy attack, the Commission is authorized during the state of war or period of national disaster due to enemy attack to employ individuals and to permit individuals access to Restricted Data pending the investigation report, and determination required by section 145b, to the extent that and so long as the Commission finds that such action is required to prevent impairment of its activities in furtherance of the common defense and security.

Sec. 161. General provisions. In the performance of its functions the Commission is authorized to:

(a) Establish advisory boards to advise with and make recommendations to the Commission on legislation, policies, administration, research, and other matters, provided that the Commission issues regulations setting forth the scope, procedure, and

limitations of the authority of each such board;

(b) Establish by rule, regulation, or order, such standards and instructions to govern the possession and use of special nuclear material, source material, and byproduct material as the Commission may deem necessary or desirable to promote the common defense and security or to protect health or to minimize danger to life or property;

(c) Make such studies and investigations, obtain such information, and hold such meetings or hearings as the Commission may deem necessary or proper to assist it in exercising any authority provided in this chapter, or in the administration or enforcement of this Act, or any regulations or orders issued thereunder. For such purposes the Commission is authorized to administer oaths and affirmations, and by subpoena to require any person to appear and testify, or to appear and produce documents, or both, at any designated place. Witnesses subpoenaed under this subsection, shall be paid the same fees and mileage as are paid witnesses in the district courts of the United States.

\* \* \* \* \*

(i) Prescribe such regulations or orders as it may deem necessary (1) to protect Restricted Data received by any person in connection with any activity authorized pursuant to this Act, (2) to guard against the loss or diversion of any special nuclear material acquired by any person pursuant to section 53 or produced by any person in connection with any activity authorized pursuant to the Act, to prevent any use or disposition thereof which the Commission may determine to be inimical to the common defense and security, including regulations or orders designating activities, involving quantities of special nuclear material which in the opinion of the Commission are important to the common defense and security, that may be conducted only by persons whose character, associations, and loyalty shall have been investigated under standards and specifications established by the Commission and as to whom the Commission shall have determined that permitting each such person to conduct the activity will not be inimical to the common defense and security, and (3) to govern any activity authorized pursuant to this Act, including standards and restrictions governing the design, location, and operation of facilities used in the conduct of such activity, in order to protect health and to minimize danger to life or property;

\* \* \* \* \*

(n) Delegate to the General Manager or other officers of the Commission any of those functions assigned to it under this Act except those specified in sections 51, 57b, 61,

108, 123, 145b (with respect to the determination of those persons to whom the Commission may reveal Restricted Data in the national interest), 145f, and 161a;

\* \* \* \* \*

(p) Make, promulgate, issue, rescind, and amend such rules and regulations as may be necessary to carry out the purposes of this Act.

APPENDIX B TO SUBPART A OF PART 710—ADJUDICATIVE GUIDELINES APPROVED BY THE PRESIDENT IN ACCORDANCE WITH THE PROVISIONS OF EXECUTIVE ORDER 12968

(The following guidelines, included in this subpart for reference purposes only, are reproduced as provided to the DOE by the Security Policy Board. The President may change the guidelines without notice.)

ADJUDICATIVE GUIDELINES FOR DETERMINING ELIGIBILITY FOR ACCESS TO CLASSIFIED INFORMATION

1. *Introduction.* The following adjudicative guidelines are established for all U.S. government civilian and military personnel, consultants, contractors, employees of contractors, licensees, certificate holders or grantees and their employees and other individuals who require access to classified information. They apply to persons being considered for initial or continued eligibility for access to classified information, to include sensitive compartmented information and special access programs and are to be used by government departments and agencies in all final clearance determinations.

2. *The Adjudicative Process.*

(a) The adjudicative process is an examination of a sufficient period of a person's life to make an affirmative determination that the person is eligible for a security clearance. Eligibility for access to classified information is predicated upon the individual meeting these personnel security guidelines. The adjudicative process is the careful weighing of a number of variables known as the whole person concept. Available, reliable information about the person, past and present, favorable and unfavorable, should be considered in reaching a determination. In evaluating the relevance of an individual's conduct, the adjudicator should consider the following factors:

- (1) The nature, extent, and seriousness of the conduct;
- (2) The circumstances surrounding the conduct, to include knowledgeable participation;
- (3) The frequency and recency of the conduct;

(4) The individual's age and maturity at the time of the conduct;

(5) The voluntariness of participation;

(6) The presence or absence of rehabilitation and other pertinent behavioral changes;

(7) The motivation for the conduct;

(8) The potential for pressure, coercion, exploitation, or duress; and

(9) The likelihood of continuation or recurrence.

(b) Each case must be judged on its own merits, and final determination remains the responsibility of the specific department or agency. Any doubt as to whether access to classified information is clearly consistent with national security will be resolved in favor of the national security.

(c) The ultimate determination of whether the granting or continuing of eligibility for a security clearance is clearly consistent with the interests of national security must be an overall common sense determination based upon careful consideration of the following, each of which is to be evaluated in the context of the whole person concept, as explained further below:

(1) Guideline A: Allegiance to the United States;

(2) Guideline B: Foreign influence;

(3) Guideline C: Foreign preference;

(4) Guideline D: Sexual behavior;

(5) Guideline E: Personal conduct;

(6) Guideline F: Financial considerations;

(7) Guideline G: Alcohol consumption;

(8) Guideline H: Drug involvement;

(9) Guideline I: Emotional, mental, and personality disorders;

(10) Guideline J: Criminal Conduct;

(11) Guideline K: Security violations;

(12) Guideline L: Outside activities;

(13) Guideline M: Misuse of Information Technology Systems.

(d) Although adverse information concerning a single criterion may not be sufficient for an unfavorable determination, the individual may be disqualified if available information reflects a recent or recurring pattern of questionable judgment, irresponsibility, or emotionally unstable behavior. Notwithstanding, the whole person concept, pursuit of further investigation may be terminated by an appropriate adjudicative agency in the face of reliable, significant, disqualifying, adverse information.

(e) When information of security concern becomes known about an individual who is currently eligible for access to classified information, the adjudicator should consider whether the person:

(1) Voluntarily reported the information;

(2) Was truthful and complete in responding to questions;

(3) Sought assistance and followed professional guidance, where appropriate;

(4) Resolved or appears likely to favorably resolve the security concern;